UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/074,124	02/12/2002	Lee Ming Cheng	P-370.240	7727

7590 01/27/2006

JACKSON WALKER L.L.P.
Suite 2100
112 E. Pecan Street
San Antonio, TX 78205

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/074,124	CHENG ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Original application contained claims 1 – 10. Claims 1, 2 and 7 have been amended in an amendment filed on 12/15/2005. The amendment filed including the specification, drawing and the claims have been entered and made of record. Presently, pending claims are 1 – 10.

Response to Arguments

2. Applicant's arguments with respect to instant claims have been fully considered but are moot in view of the new ground(s) of rejection necessitated by amendments.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claim 7 is rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 12 of copending application 09/837,981 (with the notice of allowability submitted). Although the conflicting claims are not identical, they are not patentably distinct from each other because Claim 7 of the instant application are envisioned by patented copending application claim in that claim 12 of the patented copending application contains all the limitations of claim 7 of the instant application.

In summary, Examiner notes claim 12 of patented copending application 09/837,981 recites the crypto-engine includes a randomizer and a non-linear manipulator. The linear feed back shift register as recited in claim 7 of the instant application is the most obvious type of the randomizer (which is also disclosed in the prior art section of the specification Line 13 – 24 of the patented copending application). The nonlinear function generator as recited in claim 7 of the instant application is equivalent to the non-linear manipulator as recited in claim 12 of the patented copending application. The third multiplexer as recited in claim 12 of the patented

copending application supports the function of claim limitation "randomly selecting an output sequence from one of the second plurality of binary sequences" as recited in claim 7 of the instant application.

Therefore, Claim 7 of the instant application is not patently distinct from the earlier patented copending application claim and as such is unpatentable for obvious-type double patenting.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 1 and 2 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 is indefinite because of the following reasons:

- the claim language "a second plurality of binary sequences" is not supported by the first plurality of binary sequence. The claim language "to generate a plurality of binary sequence" should be corrected as "to generate a first plurality of binary sequence".
- the claim language "to the first bit of the shift register" is not clear it is referred to "a controller including a shift register" or "a plurality of linear feedback shift registers" as recited previously.

- the claim citation of "a plurality of nonlinear function generators having said binary sequences as their input" is not clear how to map the binary sequences into the plurality of nonlinear function generators – i.e., either (a) each bit of binary sequence feeds into each separate of plurality of nonlinear function generators or the whole binary sequence equally feeds into each of the plurality of nonlinear function generators. (Also correct claim 2 with the same issue).

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claim 1, 2 and 10 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

The claim limitation of claim 1 "to select one of said second plurality of binary sequences to the first bit of the shift register, and the second switch operative to select one of said second plurality of binary sequences to an output" is not enabled by the specification. As understood by the examiner, it is not clearly pointed out how to form the K1 and K2 in order to select one of said second plurality of binary sequences

according to the specification [0035] and the Figure 5. Therefore, the invention of claim limitation is not clearly and concisely specified in a manner, which can be carried out by one skilled in the art to implement K1 and K2. (Also correct claim 2 with the same issue).

The claim limitation of claim 10 "the output sequence is randomly selected by applying one of the second plurality of binary sequences to a shift register" is not enabled by the specification. As understood by the examiner, the output sequence is randomly selected from one of the second plurality of binary sequences the according to the specification (PN 2003/0152221: Para [0015]). Therefore, the invention of claim limitation is not clearly and concisely defined / specified in a manner which can be carried out by one skilled in the art.

Any other claims not addressed are rejected by virtue of their dependency should also be corrected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 7 – 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beker (Patent Number: 4748576), in view of Roth (Patent Number: 5243650).

As per claim 7, Becker teaches a method of generating a pseudo random sequence in a sequence generator having a plurality of linear feedback shift registers and nonlinear function generators, the method comprising:

randomly selecting an output sequence from one of the second plurality of binary sequences (Beker: Figure 1: (a) The second plurality of binary sequences is equivalent to the input of the 32 – to – 1 multiplexer labeled as "Data Inputs" in Figure 1 (b) The random number of an Address Input of the 32 – to – 1 multiplexer randomly selects the output).

However, Becker does not expressly disclose how to generate each bit of the second plurality of binary sequences – i.e. the input of the 32 – to – 1 multiplexer labeled as "Data Inputs" in Figure 1. Roth teaches a secure mechanism to generate each bit of the second plurality of binary sequences (Roth: Figure 5: each bit of the second plurality of binary sequences can be generated and substituted by the functional block diagram described in Figure 5 of Roth).

In the linear feedback shift registers, generating a first plurality of binary sequences (Roth: Figure 5 and Becker Figure 1: each bit of the second plurality of binary sequences is derived from the linear feedback shift registers and thereby it constitutes a first plurality of binary sequences corresponding to the second plurality of binary sequences).

In the nonlinear function generators, applying a plurality of nonlinear functions to said first plurality of binary sequences to obtain an uncorrelated second plurality of binary sequences (Roth: Figure 5 and Becker Figure 1: each bit of the second plurality of binary sequences is further derived from a nonlinear function after the LFSR as shown (Roth: Figure 5) and thereby it constitutes a plurality of nonlinear functions to said first plurality of binary sequences).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Roth within the system of Beker because Roth teaches providing a more secure pseudo-random binary sequence generators by compensating a commonly used LFSR with a non-linear function to generate a less predictable random sequence.

As per claim 8, Becker as modified teaches the nonlinear functions are arranged to provide a one-to-many relationship between the first and second plurality of binary sequences (Beker: Figure 1: the second plurality of binary sequences is equivalent to the input of the 32 – to – 1 multiplexer labeled as "Data Inputs" in Figure 1).

As per claim 9, Becker as modified teaches the nonlinear functions are boolean functions (Roth: Column 3 Line 46 – 52 & Claim-4: the nonlinear functions comprises a XOR adder).

As per claim 10, Becker as modified does not teach the output sequence is randomly selected by applying one of the second plurality of binary sequences to a shift register (Roth: Figure 5 and Becker Figure 1: the random number of an Address Input of the 32 – to – 1 multiplexer randomly selects the output).

7. Claims 1 – 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beker (Patent Number: 4748576), in view of Roth (Patent Number: 5243650), and in view of Puhl (Patent Number: 5365585).

As per claim 1 and 2, Roth teaches a sequence generator including:

a plurality of linear feedback shift registers operable to generate a plurality of binary sequences (Beker: Figure 1),

at least first and second switches (Beker: Figure 1 and Figure 3: MUX is equivalent to a switch and Beker discloses 1st MUX (Figure 1) represented as the second switch and 2nd MUX (Figure 3) represented as the first switch);

a controller including a shift register operable to control said first and second switches (Beker: Figure 1 and Figure 3: the controller of Figure 1 is on the LEFT of the figure and the controller of Figure 3 is on the TOP of the figure);

the second switch operative to select one of said second plurality of binary sequences to an output (Beker: Figure 1: select one out of 32 of a plurality of binary sequences to an output);

Beker does not disclose expressly a plurality of nonlinear functions having said binary sequences as their input and operable to generate a second plurality of binary sequences;

Roth teaches a plurality of nonlinear functions having said binary sequences as their input and operable to generate a second plurality of binary sequences (Roth: Figure 5, Column 3 Line 46 – 52 and Claim-4: the nonlinear functions comprises XOR adder from a plurality of LFSRs as well as a nonlinear feedback shift register);

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Roth within the system of Beker because Roth teaches providing an effective encryption mechanism by using a pseudo random binary sequence generated with a nonlinear feedback register initialized by a control word where the control word in turn is generated by a true random sequence generator (Roth: Abstract).

Beker as modified does not disclose expressly the first switch operative to select one of said second plurality of binary sequences to the first bit of the shift register.

Puhl teaches the first switch operative to connect / apply the output of switch into the first bit of the shift register (Puhl: Figure 2 Element 268).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Puhl within the system of Roth as modified because Puhl teaches providing a more secure pseudo-random binary sequence generators by using an internal control mechanism which is easy to implement (Puhl: Column 1 – 3 and Column 5 Line 34 – 37).

Accordingly, Becker as modified teaches the first switch operative to select one of said second plurality of binary sequences to the first bit of the shift register (Puhl: Figure 2 Element 268; Beker: Figure 3: connecting the output of switch / MUX into the input of controller – i.e. LOAD signal as shown in Beker's Figure 3; Roth: Figure 5).

As per claim 3, Roth further teaches the sequence generator includes a plurality of feedback shift registers each operable to generate a binary sequence (Roth: Figure 5).

As per claim 4, Roth further teaches the nonlinear function generators includes a plurality of boolean functions, each boolean function having the first plurality of binary sequences as an input and being operable to generate a binary sequence (Roth: Column 3 Line 46 – 52 & Claim-4: the nonlinear functions comprises a XOR adder from a plurality of LFSRs and a nonlinear shift register).

As per claim 5, Beker further teaches the switches are multiplexers (Beker: Figure 1).

As per claim 6, Roth as modified further teaches the controller includes a shift register, the input of the controller being the first bit of the register and the outputs of the controller being at positions along the register (Puhl: Figure 2 Element 268; Beker:

Figure 3: connecting the output of switch / MUX into the input of controller – i.e. LOAD signal as shown in Beker's Figure 3; Roth: Figure 5).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100